

# **EXHIBIT U**

**EXHIBIT F-10**

**Invalidity Claim Chart for U.S. Patent No. 8,141,154 based on Symantec/IBM Digital Immune System  
("Digital Immune System")**

**Grounds**

Claims 1, 2, 4, 6, 7, 10 of the '154 patent are rendered obvious by Digital Immune System alone or in combination with VirusWall, AppletTrap, Janus System, Shipp, Khazan, Chander, Sirer or Davis.

**Prior Art Status**

Digital Immune System was publicly available at least as early as October 1997 and is prior art under at least 35 U.S.C. §§ 102(a) and (b), as elaborated in the following:

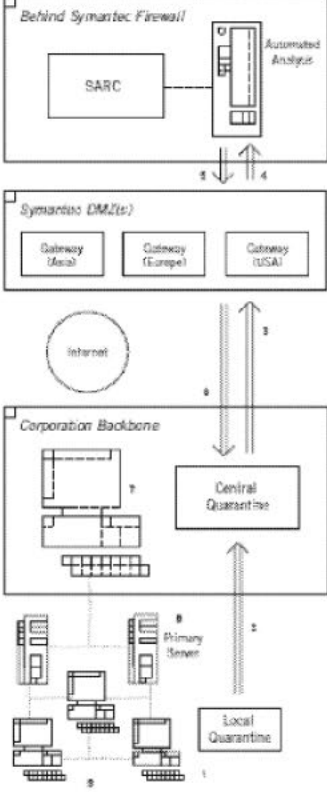
- "The Digital Immune System, Enterprise-Grade Anti-Virus Automation In the 21st century," Symantec Technical Brief (2001) (hereinafter, "Symantec"), "Blueprint for a Computer Immune System," by Kephart et al., Proceedings of the Seventh International Virus Bulletin Conference, October 1997, Virus Bulletin Ltd.
- Artificial Immune Systems and their Applications by Springer-Verlag Berlin Heidelberg, 1999 (hereinafter, "Blueprint"), which was published in October 1997.
- "A Biologically Inspired Immune System for Computers," by Kephart, Artificial Life IV, R. Brooks and P. Maes, eds., MIT Press, 1994 (hereinafter, "Biologically Inspired"), which was published in 1994.
- "Biologically Inspired Defenses Against Computer Viruses," by Kephart et al., International Joint Conferences on Artificial Organization (IJCAI), Proceedings of the Fourteenth International Joint Conference on Artificial Intelligence (I), Montreal, Quebec, Canada, August 20-25, 1995 (hereinafter, "Inspired Defenses").
- U.S. Patent No. 5,440,723 issued to Arnold et al. (hereinafter, "Arnold"), which was filed on January 19, 1993, issued on August 8, 1995.



<u>'154 Patent</u>	<u>Digital Immune System Alone or In Combination with Other Prior Art</u>
<u>Claim 1</u>	
	Abstract.)
<p>[a] a content processor (i) for processing content received over a network, the content including a call to a first function, and the call including an input, and (ii) for invoking a second function with the input, only if a security computer indicates that such invocation is safe;</p>	<p>Digital Immune discloses this element and/or renders it obvious either alone or in combination with other references and/or the knowledge of one of ordinary skill in the art.</p> <p>Digital Immune discloses a content processor (i) for processing content received over a network, the content including a call to a first function, and the call including an input, and (ii) for invoking a second function with the input, only if a security computer indicates that such invocation is safe. Digital immune detects new or unknown threats at the desktop, server, and gateway level. Symantec at p. 5. Digital Immune discloses that “[f]irst, it checks to see if it can handle the sample by itself. It does this by trying to match a checksum of the sample file with a database of checksums that correspond to previously analyzed files - files that are known to be clean and files known to contain a particular virus. If a match is found, a result is returned indicating that the file is not infected, or that it is known to be infected and can be handled with a virus definition set of a particular version or later.” Inspired Defenses at Fig. 3. The initial check is the claimed first function, and the handling of a result if a file is not infected is the claimed second function. The described “application capable of interpreting and displaying” content is the claimed content processor. Inspired Defenses at Fig. 3. The location where a packaged sample is sent is the claimed security computer. Anatomy at pp. 11-12 (“a sample of the suspicious object is extracted, packaged in a harmless form, and sent off to an anti-virus administrator system over the organization’s internal network”). Further citations below corroborate this functionality.</p> <p>“IBM® and Symantec designed the Digital Immune System as a closed-loop automated system to deal with Melissa-class threats, orders-of-magnitude increases in submissions, floods, and denial-of-service attacks. The Digital Immune System:</p> <p>11. Detects a high percentage of new or unknown threats at the desktop, server, and</p>



<u>'154 Patent</u>	<u>Digital Immune System Alone or In Combination with Other Prior Art</u>
<u>Claim 1</u>	
	<p>gateway.</p> <p>12. Makes the full system highly scalable.</p> <p>13. Provides secure submission of virus samples and secure distribution of new definitions.</p> <p>14. Provides intelligent filtering of submissions to focus system resources on the most critical threats.</p> <p>15. Provides high-speed analysis capabilities.</p> <p>16. Reduces instances of false positives.</p> <p>17. Provides full end-to-end automation of submission, analysis, and distribution of new definitions.</p> <p>18. Provides real-time status updates on all submissions.</p> <p>19. Manages common flooding conditions and denial of service attacks.</p> <p>20. Provides the administrator with the ability to set the level of automation.”</p> <p>(Symantec at p. 4.)</p> <p>“The first step in building an automated anti-virus analysis and response system is detecting new or unknown threats at the desktop, the server, and the gateway. Suspicious files can then be forwarded for automatic analysis and processing.” (Symantec at p. 5.)</p>

'154 Patent	<b>Digital Immune System Alone or In Combination with Other Prior Art</b>
<b>Claim 1</b>	
	 <p>The diagram illustrates the Digital Immune System architecture. It shows a local quarantine (1) connected to a primary server (8) and a local quarantine (9). The primary server (8) is connected to a corporate backbone (7) which contains a central quarantine (7). The corporate backbone (7) is connected to a Symantec DMZ (6) which contains three gateways (Gateway (Local), Gateway (Europe), Gateway (USA)). The Symantec DMZ (6) is connected to the Internet (5). The Internet (5) is connected to a SARC (3) and an Automated Analysis (4) unit. The SARC (3) is connected to the Automated Analysis (4) unit. The Automated Analysis (4) unit is connected to the Internet (5). The Internet (5) is connected to the Symantec DMZ (6). The Symantec DMZ (6) is connected to the Corporate Backbone (7). The Corporate Backbone (7) is connected to the Primary Server (8). The Primary Server (8) is connected to the Local Quarantine (9). The Local Quarantine (9) is connected to the Primary Server (8). The Primary Server (8) is connected to the Local Quarantine (9). The Local Quarantine (9) is connected to the Primary Server (8). The Primary Server (8) is connected to the Local Quarantine (9). The Local Quarantine (9) is connected to the Primary Server (8).</p> <ol style="list-style-type: none"> <li>1. New/unknown viruses quarantined</li> <li>2. Local quarantine forwards samples to corporate quarantine</li> <li>3. Corporate quarantine securely forwards samples to regional Symantec gateway</li> <li>4. Gateway forwards samples to back-end automation</li> <li>5. Back-end automation forwards new cure/fingerprints to gateway</li> <li>6. Gateways securely forward status and fingerprints to corporate quarantine</li> <li>7. Corporate quarantine forwards fingerprints to master management server</li> <li>8. Master servers automatically forward samples to primary servers</li> <li>9. Primary servers roll out definitions to clients</li> </ol> <p>Figure 3: The Digital Immune System. All numbered pathways are automatic and require no user intervention.</p> <p>(Symantec, Fig. 3.)</p> <p>“Norton AntiVirus™ automatically isolates potential new or unknown viruses in a local</p>





<u>'154 Patent</u>	<u>Digital Immune System Alone or In Combination with Other Prior Art</u>
<u>Claim 1</u>	
	<p>quarantine on the desktop, server, or gateway. Norton AntiVirus automatically forwards these suspected infections from the local quarantine to the corporate Central Quarantine.” (Symantec at p. 6.)</p> <p>“From corporate quarantine, administrators can examine all infected files, select the desired automated operations, or manually submit files to Symantec Security Response.” (Symantec at p. 6.)</p> <p>“When a submission must be sent on to Symantec Security Response, and when configured to do so, Central Quarantine automatically encrypts and sends the submission using the Digital Immune System.” (Symantec at p. 6.)</p> <p>“UPON RECEIVING A NEW SUBMISSION, THE BACK-END AUTOMATION SYSTEM:</p> <ol style="list-style-type: none"> <li>1. Tracks the submission in a database.</li> <li>2. Filters files in the submission to reduce manual processing.</li> <li>3. Attempts replication of suspect document and spreadsheet files to generate cures for new and unknown macro and DOS viruses.</li> <li>4. Prioritizes submissions that must be handled manually.</li> <li>5. Responds to customers with status data, resolution information, and fingerprints.” (Symantec at p. 8.)</li> </ol> <p>“To see how this immune system functions, we now step through an example of detecting a virus at a client system, sending a sample of the virus to a local administrator, transporting it to a virus analysis center, analyzing it, and distributing the cure.” (Anatomy at p. 10.)</p> <p>“A possibly new virus is detected on a client system. This is done by an anti-virus product on that system, and can be done in a number of ways. Heuristics can detect a new, previously unknown virus either by its appearance, by simulating how it will behave when</p>